
Damian Krawczyk

Wydanie 0.0.1

Damian Krawczyk

13 sty 2023

1	o mnie	3
2	projekty	5
2.1	GPI - GOV PL Info	6
2.1.1	Dla kogo	6
2.1.2	Jak to działa	7
2.1.3	Jak subskrybować	7
2.1.4	Lista kanałów	7
2.1.5	Stack technologiczny	7
2.1.6	Kontakt	8
2.2	LimberDuck.org	10
2.2.1	nessus file analyzer	12
2.2.2	nessus file reader	13
2.2.3	converter csv	14
3	notes	15
3.1	Apple Automator	15
3.1.1	Quick Actions	15
3.2	Insert current date and time	17
3.2.1	Visual Studio Code	17
3.3	Test note	17
4	zakładki	19
4.1	dokumentacja	19
4.1.1	changelog	19
4.1.2	Sphinx	19
4.1.3	wersjonowanie	19
4.2	języki programowania	20
4.2.1	python	20
4.3	systemy kontroli wersji	20
5	skrót	21
6	kontakt	23
7	słownik	25

LimberDuck.org

Narzędzia dla inżynierów i menedżerów cyberbezpieczeństwa do automatyzacji pracy.

PROJEKTY

Kliknij tutaj, aby zobaczyć moje projekty.

NOTATKI

Kliknij tutaj, aby zobaczyć moje notatki.

ZAKŁADKI

Kliknij tutaj, aby zobaczyć interesujące zakładki

SKRÓTY

Kliknij tutaj, aby zobaczyć przydatne skróty.

Jestem entuzjastą **automatyzacji**, zarówno w moim życiu prywatnym oraz zawodowym. Głównym powodem tego jest CZAS - jedna z najcenniejszych rzeczy jaką posiadamy. Współczesna technologia pozwala nam projektować i wdrażać przyjazne dla użytkownika rozwiązania, które znacząco mogą poprawić sposób w jaki na co dzień żyjemy lub pracujemy. Podstawą tych rozwiązań są DANE - następna cenna rzecz, która wymaga jednak odpowiedniej ochrony. **Bezpieczeństwo Informacji** (ang. **Information Security**)¹ to dziedzina zajmująca się ochroną danych i jest ona moim kolejnym zainteresowaniem. Powinno ono być brane pod uwagę podczas prac nad każdym produktem, już na początkowym etapie jego tworzenia oraz odpowiednio utrzymywane w trakcie całego cyklu życia produktu. Mam przyjemność zajmować się obiema kwestiami pracując jako **Inżynier Bezpieczeństwa** (ang. **Security Engineer**) oraz **Inżynier DevOps** (ang. **DevOps Engineer**). Jestem odpowiedzialny za utrzymywanie i rozwój procesu **Vulnerability Assessment**² przez większość mojej kariery zawodowej.

Promuję otwarty sposób pracy. Z punktu widzenia oprogramowania oznacza to, że jeśli to możliwe, moje rozwiązania udostępniam w formie **Otwartego oprogramowania** (ang. **Open Source**)³ lub **Otwartego oprogramowania w obrębie organizacji** (ang. **Inner Source**)⁴. Mam nadzieję, że projekty, którymi się tutaj podzielę okażą się przydatne również dla Ciebie.

¹ *Information Security*

² *Vulnerability Assessment*

³ *Open Source*

⁴ *Inner Source*

projekty

Sprawdź moje *projekty*.

kontakt

Tutaj *kontakt* do mnie.

GPI - GOV PL Info



GPI - GOV PL Info jest projektem zainicjowanym 1 kwietnia 2021 roku. Głównym celem tego projektu jest dostarczenie informacji wysyłanych przez Rząd Polski w formie notyfikacji mobilnych, poprzez wykorzystanie [Kanałów aplikacji Telegram](#), w językach polskim oraz angielskim.

[przeczytaj więcej](#)

LimberDuck.org



LimberDuck (wym. lm.b dk) jest projektem rozpoczętym 26 listopada 2018 roku. Głównym celem tego projektu jest stworzenie zestawu darmowych narzędzi Open Source¹ dedykowanych dla Inżynierów Bezpieczeństwa (ang. Security Engineers), którzy chcą zautomatyzować swoją pracę, zmniejszyć obciążenie zadaniami oraz skupić na analizie danych.

[przeczytaj więcej](#)

¹ [przeczytaj więcej o Open Source](#) w słowniku

2.1 GPI - GOV PL Info



GPI - GOV PL Info jest projektem zainicjowanym 1 kwietnia 2021 roku. Głównym celem tego projektu jest dostarczenie informacji wysyłanych przez Rząd Polski w formie notyfikacji mobilnych. Zostało to osiągnięte w prosty sposób poprzez wykorzystanie [Kanałów aplikacji Telegram](#). Ponieważ źródło informacji jest udostępniane w języku polskim, wszystkie notyfikacje są również wysyłane w języku polskim. Dodatkowo jednak są one w automatyczny sposób tłumaczone na język angielski przy wykorzystaniu usługi Translatora Google co powinno sprawić, że życie obcokrajowców w Polsce stanie się odrobinę łatwiejsze.

2.1.1 Dla kogo

To rozwiązanie jest dedykowane **dla każdego kto dba o swoje zdrowie** i chce otrzymywać takie informacje jak:

- **ostrzeżenia o produktach spożywczych oraz produktach codziennego użytku wycofanych ze sprzedaży** w Polsce z różnych powodów związanych ze zdrowiem i bezpieczeństwem opublikowane przez Główny Inspektorat Sanitarny w Polsce (GIS (Główny Inspektorat Sanitarny)),
- **ostrzeżenia o lekach wycofanych ze sprzedaży** w Polsce z różnych powodów związanych ze zdrowiem i bezpieczeństwem opublikowane przez Główny Inspektorat Farmaceutyczny w Polsce (GIF (Główny Inspektorat Farmaceutyczny)),
- komunikatach i **działaniach Rządu Polski dotyczących koronawirusa / COVID-19**.

To rozwiązanie jest dedykowane **dla każdego kto dba o swój czas** i chce otrzymywać w wygodny sposób:

- powiadomienia bezpośrednio na smartfon, tablet lub komputer,
- powiadomienia w języku angielskim i języku polskim,
- powiadomienia, które można w prosty sposób przekazać dalej,
- informacje bezpośrednio ze źródła (gov.pl),
- informacje bez reklam rozpraszających uwagę,

- błyskawiczne wyszukiwanie wiadomości, której szukasz, nawet wśród milionów, np. [gluten](#), [Salmonella](#), [Pfizer](#), [Janssen](#), [AstraZeneca](#), [Tarcza antykryzysowa](#), itd.

Jak i również dla każdego kto chce dać sobie chwilę odpoczynku od takich źródeł informacji jak Facebook, Twitter, TV czy radio.

2.1.2 Jak to działa

Aktualna implementacja tego rozwiązania działa w następujący sposób:

1. Codziennie po północy pobierana jest zawartość stron [gov.pl](#).
2. Jeżeli w minionym dniu zostały na nich opublikowane artykuły Ty otrzymasz powiadomienie w aplikacji Telegram na swoim smartfonie, tablecie lub komputerze.

2.1.3 Jak subskrybować

1. Jeżeli nie masz jeszcze aplikacji Telegram, pobierz ją stąd <https://telegram.org/dl/>.
Wspierane Systemy Operacyjne: Android, iOS, iPadOS, Windows, macOS, Linux.
2. Zarejestruj się postępując zgodnie z instrukcjami wyświetlanymi na ekranie.
3. Subskrybuj Kanały GPI (GOV PL Info) w aplikacji Telegram.

Informacja:

Twój numer telefonu nie jest widoczny dla pozostałych subskrybentów!

Domyślnie Twój numer jest widoczny tylko dla osób, które dodałeś do swojej książki adresowej jako kontakty.

Przeczytaj więcej na ten temat tutaj (ang.) <https://telegram.org/faq#q-who-can-see-my-phone-number>

2.1.4 Lista kanałów

Zobacz także:

Sprawdź [LISTĘ DOSTĘPNYCH KANAŁÓW GPI W APLIKACJI TELEGRAM](#) i zasubskrybuj ten, który najbardziej Cię interesuje.

2.1.5 Stack technologiczny

python



Python został tutaj wykorzystany do napisania kodu potrzebnego do pobierania danych z wybranych podstron [gov.pl](#), przeparasowania ich, znalezienia artykułów, które zostały ostatnio opublikowane, przetłumaczenia ich za pomocą usługi Tłumacz Google i wreszcie przygotowania ich do wysłania do utworzonych wcześniej Kanałów w aplikacji Telegram.

GPI kod źródłowy	https://github.com/damian-krawczyk/gov-pl-info
------------------	---

GitHub Actions



GitHub Actions zostało wykorzystane do zdefiniowania workflows dla wybranych wątków z gov.pl oraz dedykowanych Kanałów w aplikacji Telegram. Każde workflow uruchamia się po północy CET (Central European Time) lub CEST (Central European Summer Time), aby pobrać artykuły udostępnione poprzedniego dnia.

GPI workflows	https://github.com/damian-krawczyk/gov-pl-info/actions
---------------	---

Telegram



Telegram jest tutaj głównym medium wykorzystywanym do dostarczenia powiadomień o artykułach znalezionych na wybranych podstronach gov.pl. Dzięki nielimitowanej ilości subskrybentów powinno być możliwe dostarczenie powiadomień do wszystkich osób mieszkających w Polsce (38 137 795 - GUS (Główny Urząd Statystyczny) 2020 - [źródło](#)). Telegram wspiera następujące Systemy Operacyjne: Android, iOS, iPadOS, Windows, macOS, Linux.

Translator Google



Translator Google jest wykorzystywany do tłumaczenia powiadomień z języka polskiego na język angielski. Powiadomienie zawierające informacje w obu językach jest wysyłane na dedykowany Kanał w aplikacji Telegram.

2.1.6 Kontakt

Ważne: Napotkałeś jakikolwiek problem korzystając z tego rozwiązania?

Zauważyłeś błąd?

Chciałbyś, żebym stworzył dla Ciebie podobne rozwiązanie dopasowane do Twoich potrzeb?

Daj mi o tym znać!

SZCZEGÓŁY KONTAKTU

Kanały GPI

Uwaga: Kanały w aplikacji Telegram wymienione poniżej nie są dostarczane ani również wspierane przez Rząd Polski.

Główny Inspektorat Sanitarny

GIS - Główny Inspektorat Sanitarny w Polsce dostarcza informacje na stronie internetowej <https://www.gov.pl/web/gis> poprzez wątki:

- Wiadomości
- Ostrzeżenia

Informacje z wątku **Ostrzeżenia** są przesyłane na Kanał aplikacji Telegram wskazany poniżej.



[KLIKNIJ ABY SUBSKRYBOWAĆ](#) Kanał GPI GIS w aplikacji Telegram

Wskazówka: Kliknij w [Preview Channel](#), aby zobaczyć zawartość Kanału.

Główny Inspektorat Farmaceutyczny

GIF - Główny Inspektorat Farmaceutyczny w Polsce publikuje decyzje na stronie internetowej RDG <https://rdg.ezdrowie.gov.pl> oraz na głównej stronie internetowej <https://www.gov.pl/web/gif> poprzez wątki:

- Wiadomości
- Interpretacje
- Komunikaty

Decyzje oraz informacje z wątku **Wiadomości** są przesyłane na Kanał aplikacji Telegram wskazany poniżej.



[KLIKNIJ ABY SUBSKRYBOWAĆ](#) Kanał GPI GIF w aplikacji Telegram

Wskazówka: Kliknij w [Preview Channel](#), aby zobaczyć zawartość Kanału.

Koronawirus

Rząd Polski dostarcza informacje związane z koronawirusem na stronie internetowej <https://www.gov.pl/web/koronawirus> poprzez wątki:

- Działania rządu
- Komunikaty

Informacje z tych wątków są przesyłane na Kanał aplikacji Telegram wskazany poniżej.



[KLIKNIJ ABY SUBSKRYBOWAĆ](#) Kanał GPI Koronawirus w aplikacji Telegram

Wskazówka: Kliknij w [Preview Channel](#), aby zobaczyć zawartość Kanału.

GPI Health Check Channel

Ten Kanał w aplikacji Telegram dostarcza informacje o braku artykułów na dany dzień. Zachęcam do subskrypcji tego Kanału oraz jego wyciszenia ponieważ w przypadku braku artykułów notyfikacje pojawiają się tam codziennie.



[KLIKNIJ ABY SUBSKRYBOWAĆ](#) Kanał GPI Health Check w aplikacji Telegram

Wskazówka: Kliknij w [Preview Channel](#), aby zobaczyć zawartość Kanału.

Wskazówka: Sprawdź jak wyciszyć Kanał w aplikacji Telegram [tutaj](#).

2.2 LimberDuck.org



LimberDuck (wym. lm.b dk) jest projektem rozpoczętym 26 listopada 2018 roku. Głównym celem tego projektu jest stworzenie zestawu darmowych narzędzi Open Source¹ dedykowanych dla Inżynierów Bezpieczeństwa (ang. Security Engineers), którzy chcą zautomatyzować swoją pracę, zmniejszyć obciążenie zadaniami oraz skupić się na analizie danych.

Tabela 1: szczegóły projektu LimberDuck

strona główna	https://limberduck.org
strona GitHub	https://github.com/limberduck

Narzędzia

nessus file analyzer



Jest to narzędzie z graficznym interfejsem użytkownika (ang. GUI (Graphical User Interface)), które pozwala na analizę plików nessus zawierających wyniki skanów wykonanych za pomocą aplikacji *Nessus* lub *Tenable.sc* wydanych przez © Tenable, Inc. które to aplikacje często wykorzystywane są w procesie VA (Vulnerability Assessment)².

przeczytaj więcej

nessus file reader



Jest to moduł pythonowy pozwalający na szybkie parsowanie plików nessus zawierających wyniki skanów wykonanych za pomocą aplikacji *Nessus* lub *Tenable.sc* wydanych przez © Tenable, Inc. które to aplikacje często wykorzystywane są w procesie VA².

przeczytaj więcej

¹ przeczytaj więcej o *Open Source* w słowniku

² przeczytaj więcej o *Vulnerability Assessment* w słowniku

converter csv



Jest to narzędzie z graficznym interfejsem użytkownika (ang. GUI), które pozwala na konwersję wielu plików csv (comma-separated value) o dużych rozmiarach do plików xlsx (Microsoft Excel Open XML Spreadsheet), utrzymując wykorzystanie pamięci operacyjnej na niskim poziomie.

przeczytaj więcej

2.2.1 nessus file analyzer



Jest to narzędzie z graficznym interfejsem użytkownika (ang. GUI), które pozwala na konwersję wielu plików nessus zawierających wyniki skanów wykonanych za pomocą aplikacji *Nessus* lub *Tenable.sc* wydanych przez © Tenable, Inc. które to aplikacje często wykorzystywane są w procesie VA¹. Przeparsowane wyniki skanów są eksportowane do arkusza kalkulacyjnego Microsoft Excel (xlsx) ułatwiając ich analizę.

Wykorzystanie pamięci operacyjnej będzie utrzymywane na niskim poziomie nawet podczas parsowania plików o dużym rozmiarze. Narzędzie to można uruchomić na systemach operacyjnych Windows, MacOS czy GNU Linux. Wynikiem działania jest arkusz kalkulacyjny Microsoft Excel (xlsx) z zakładkami zawierającymi kolejno dane: podsumowanie całego skanu, podsumowanie wszystkich przeskanowanych hostów, wszystkie szczegółowe wyniki na temat wykrytych podatności² czy niezgodności. Jest to darmowe narzędzie Open Source³.

Tabela 2: szczegóły projektu nessus file analyzer

strona główna	https://limberduck.org/en/latest/nessus-file-analyzer
---------------	---

¹ przeczytaj więcej o *Vulnerability Assessment* w słowniku

² przeczytaj więcej o *vulnerability* w słowniku

³ przeczytaj więcej o *Open Source* w słowniku

stack technologiczny



2.2.2 nessus file reader



Jest to moduł pythonowy pozwalający na szybkie parsowanie plików nessus zawierających wyniki skanów wykonanych za pomocą aplikacji *Nessus* lub *Tenable.sc* wydanych przez © Tenable, Inc. które to aplikacje często wykorzystywane są w procesie VA¹. Moduł ten pozwala na pobranie danych poprzez funkcje zgrupowane w następujące kategorie: plik, skan, host, oraz plugin. Możliwe jest pobranie konkretnych informacji z wskazanych plików z wynikami skanów w formacie nessus np. rozmiar pliku, nazwa raportu, nazwy przeskanowanych hostów, liczba hostów podanych jako cel skanu, lista hostów przeskanowana z wykorzystaniem testów wymagającymi uwierzytelniania, liczba wykrytych podatności dla każdego współczynnika ryzyka (ang. Risk Factor), dokładny czas skanu poszczególnych hostów, właściwy wynik zwrócony przez wskazany plugin (ang. plugin output) oraz wiele innych. Jest to darmowe narzędzie Open Source².

Tabela 3: szczegóły projektu nessus file reader

strona główna	https://limberduck.org/en/latest/nessus-file-reader
---------------	---

¹ przeczytaj więcej o *Vulnerability Assessment* w słowniku

² przeczytaj więcej o *Open Source* w słowniku

stack technologiczny



2.2.3 converter csv



Jest to narzędzie z graficznym interfejsem użytkownika (ang. GUI), które pozwala na konwersję wielu plików csv o dużych rozmiarach do plików xlsx, utrzymując wykorzystanie pamięci operacyjnej na niskim poziomie. Narzędzie to można uruchomić na systemach operacyjnych Windows, MacOS czy GNU Linux. Jest to darmowe narzędzie Open Source¹.

Tabela 4: szczegóły projektu converter csv

strona główna	https://limberduck.org/en/latest/converter-csv
---------------	---

stack technologiczny



¹ przeczytaj więcej o *Open Source* w słowniku

3.1 Apple Automator



dakr.link/n2

3.1.1 Quick Actions

Open in

Open in Visual Studio Code

1. Open *Automator*
2. Go to *File > New*.
3. Choose *Quick Action*.
4. Change *Workflow Receives current* to *files or folders in Finder.app*.
5. Add a *Run Shell Script* action by drag and drop.
6. Change *Pass input* to *as arguments*
7. Copy and paste the following in the shell script box:

```
open -n -b "com.microsoft.VSCode" --args "$@"
```

8. Go to *File > Save* and save it as e.g. *Open in Visual Studio Code*.
9. Go to Finder.
10. Click RMB (right mouse button) on folder or file.
11. Choose from menu *Quick Actions > Open in Visual Studio Code*

Informacja: If you have *Path Bar* enabled in Finder (alt-cmd P) and you want to use this *Quick Action* also from *Path Bar*, click RMB on folder or file in *Path Bar* and choose from menu *Services > Open in Visual Studio Code*.

Open in Visual Studio Code, based on [jnovack post @ stackoverflow.com](#)
CC BY-SA 4.0

Open in pyCharm

1. Open *Automator*
2. Go to *File > New*.
3. Choose *Quick Action*.
4. Change *Workflow Receives current* to *files or folders in Finder.app*.
5. Add a *Run Shell Script* action by drag and drop.
6. Change *Pass input* to *as arguments*
7. Copy and paste the following in the shell script box:

```
open -n -b "com.jetbrains.pycharm" --args "$@"
```

8. Go to *File > Save* and save it as e.g. *Open in PyCharm*.
9. Go to Finder.
10. Click RMB on folder or file.
11. Choose from menu *Quick Actions > Open in PyCharm*

Informacja: If you have *Path Bar* enabled in Finder (alt-cmd P) and you want to use this *Quick Action* from *Path Bar*, click RMB on folder or file in *Path Bar* and choose from menu *Services > Open in PyCharm*

3.2 Insert current date and time



dakr.link/n1

3.2.1 Visual Studio Code

1. Install [Insert Date String](#) extension created by Jakub Synowiec.
2. Insert date and time:
 - Shift-cmd I (macOS)
 - Ctrl-Shift I (Windows/Linux)
3. Go to extension settings if you want to change format of inserted date and time and change setting named *Insert Date String: Format*:
 - YYYY-MM-DD hh:mm:ss (default value) e.g. 2021-12-30 09:07:11
 - YYYY-MM-DD hh:mm:ss ZZZZ (UTC Time offset value included) e.g. 2021-12-30 09:07:52 +0100
4. Read more in [Usage](#) instructions.

3.3 Test note



dakr.link/test-note

Test note body

[dakr.link/bookmarks](#)

Tutaj znajdziesz kilka interesujących linków. Zobacz [plik źródłowy](#) oraz [changelog](#) w GitHub'ie.

4.1 dokumentacja

4.1.1 changelog

- [keep a changelog - example how to maintain changelog](#) [en] [pl] [more]

4.1.2 Sphinx

- [my list of Sphinx related GitHub repositories](#) [en]
- [list of Sphinx extensions](#) [en]

4.1.3 wersjonowanie

- [Semantic Versioning 2.0.0](#) - set of rules and requirements that dictate how version numbers are assigned and incremented. [en] [pl] [more]

4.2 języki programowania

4.2.1 python

- strftime.org - Python strftime cheatsheet [en]

4.3 systemy kontroli wersji

- starchart.cc - plot your repository stars over time [en]
- [Shields.io](https://shields.io/) - quality metadata badges for open source projects [en]



dakr.link/shortcuts

Tutaj znajdziesz kilka przydatnych skrótów. Zobacz plik źródłowy oraz changelog w GitHub'ie.

skrót	opis	nazwa produktu	SO (System Operacyjny)
CapsLock-alt LMB	zaznaczenie pionowe	Visual Studio Code	macOS
Shift-cmd-P	paleta komend	Visual Studio Code	macOS
Shift-alt Up	skopiuj wybrane linie	Visual Studio Code	macOS
Shift-alt Down	skopiuj wybrane linie	Visual Studio Code	macOS
alt Up	przenieś wybrane linie do góry	Visual Studio Code	macOS
alt Down	przenieś wybrane linie w dół	Visual Studio Code	macOS
cmd-D	dodaj tą stronę do ulubionych	Safari, Chrome, Firefox	macOS

ROZDZIAŁ 6

kontakt

[linkedin.com/in/damian-krawczyk-in](https://www.linkedin.com/in/damian-krawczyk-in)

github.com/damian-krawczyk

damian@damiankrawczyk.com

Katowice, Polska / zdalnie

Open Source

Generally, Open Source software is software that can be freely accessed, used, changed, and shared (in modified or unmodified form) by anyone. Open source software is made by many people, and distributed under licenses that comply with the [Open Source Definition](#).

Source: <https://opensource.org/faq#osd>

Information Security

Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Source: <https://www.sans.org/information-security>

Inner Source

InnerSource takes the lessons learned from developing open source software and applies them to the way companies develop software internally. As developers have become accustomed to working on world class open source software, there is a strong desire to bring those practices back inside the firewall and apply them to software that companies may be reluctant to release. For companies building mostly closed source software, InnerSource can be a great tool to help break down silos, encourage internal collaboration, accelerate new engineer on-boarding, and identify opportunities to contribute software back to the open source world.

Source: <https://innersourcecommons.org>

vulnerability

A vulnerability /vulnrblti/ is a weakness in a system that allows a threat source to compromise its security. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

Source: *CISSP All-in-One Exam Guide, 8th Edition, 2018, by Shon Harris, Fernando Maymi, page 6*

VA**Vulnerability Assessment**

A vulnerability assessment identifies a wide range of vulnerabilities in the environment. This is commonly

carried out through a scanning tool. The idea is to identify any vulnerabilities that potentially could be used to compromise the security of our systems. By contrast, in a penetration test, the security professional exploits one or more vulnerabilities to prove to the customer (or your boss) that a hacker can actually gain access to company resources.

Source: CISSP All-in-One Exam Guide, 8th Edition, 2018, by Shon Harris, Fernando Maymi, page 878

I

Information Security, [25](#)

Inner Source, [25](#)

O

Open Source, [25](#)

V

VA, [25](#)

vulnerability, [25](#)

Vulnerability Assessment, [25](#)